WHAT IS CLAIMED IS:

1. A monitoring/intrusion detection system, comprising:

a central loghost,

at least one proxy loghost in communication with the central loghost; and

at least one monitoring station,

wherein the proxy loghost receives a plurality of log files from a plurality of resources operating on a network, analyzes the log files for at least one of unexpected volume, unexpected patterns, or unexpected types of log files, and generates events in view of such analysis,

wherein the central loghost is operable to receive the events generated by the proxy loghost and generate an alert upon an analysis of the events, and

wherein the monitoring station is caused to issue an alarm when the alert is generated.

2. The system of claim 1, wherein the central loghost comprises a plurality modules operating in a Unix environment.

3. The system of claim 1, further comprising a plurality of proxy loghosts, each one of the pluraility being in communication with the central loghost.

4. The system of claim 1, wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer.

5. The system of claim 1, wherein a plurality of events is required to cause the generation of an alert.

6. The system of claim 1, wherein security management has access to both the proxy loghost and the central loghost.

7. The system of claim 1, wherein the log files are received from a network-based intrusion detection system.

8. The system of claim 1, wherein the log files are received from a host-based intrusion detection system.

9. The system of claim 1, wherein the log files are archived on the proxy loghost and the events are archived on the central loghost.

10. The system of claim 1, further comprising software adapters to convert one format of a log file to another format.

11. The system of claim 1, further comprising a module for visualizing the log files received at the proxy loghost.

12. A system for detecting intrusion into a secure network, comprising:

a plurality of proxy loghosts, each proxy loghost collecting log files that are generated by resources in a portion of the secure network, the plurality of loghosts generating events in response to the log files collected; and

a central loghost in communication with the plurality of proxy loghosts, the central loghost receiving at least one of (i) the log files themselves and (ii) the events from the plurality of proxy loghosts, the central loghost analyzing the events to determine the necessity of generating an alert and an associated alarm to notify a security manager of a possible intrusion incident.

13. The system of claim 12, wherein the central loghost comprises a plurality modules operating in a Unix environment.

14. The system of claim 12, wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer.

15. The system of claim 12, wherein a plurality of events is required to cause the generation of an alert.

16. The system of claim 12, wherein security management has access to both the plurality of proxy loghosts and the central loghost.

17. The system of claim 12, wherein the log files are received from a network-based intrusion detection system.

18. The system of claim 12, wherein the log files are received from a host-based intrusion detection system.

19. The system of claim 1, wherein the log files are archived on the plurality of proxy loghosts and events are archived on the central loghost.

20. The system of claim 12, further comprising software adapters to convert one format of a log file to another format.

21. The system of claim 12, further comprising a module for visualizing the log files received at the proxy loghost.

22. A method of monitoring a network, comprising:

receiving a plurality of log messages at a proxy loghost;

analyzing the log messages and determining whether, in the log files, there exists any anomalies or unusual patterns;

generating an event in response to the anomalies or unusual patterns and forwarding the event to a central loghost;

monitoring the events at the central loghost and generating an alert in accordance with predetermined event analysis; and

sounding an alarm in coordination with the alert, the alarm being indicative of an unwanted incident in the network.

23. The method of claim 22, wherein the central loghost comprises a plurality modules operating in a Unix environment.

24. The method of claim 22, wherein a plurality of proxy loghosts receive log files.

25. The method of claim 22, wherein the log files are received from resources comprising at least one of an operating system, application, firewall, router, switch and loadbalancer.

26. The method of claim 22, further comprising generating the alert only after a plurality events are received.

27. The method of claim 22, further comprising remotely accessing, from a single location, both the proxy loghost and the central loghost.

28. The method of claim 22, wherein the log files are received from a network-based intrusion detection system.

29. The method of claim 22, wherein the log files are received from a host-based intrusion detection system.

30. The method of claim 22, further comprising archiving the log files on the proxy loghost and archiving the event on the central loghost.